DoD Comprehensive Military Unmanned AERIAL VEHICLE SMART DEVICE GROUND CONTROL STATION THREAT MODEL

Image designed by Diane Fleischer

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **APR 2015**	2. REPORT TYPE	3. DATES COVERED **00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE **DoD Comprehensive Military Unmanned Aerial Vehicle Smart Ddevice Ground Control Station Threat Model**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Acquisition University,9820 Belvoir Rd Ste 3,Fort Belvoir,VA,22060-9910**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**34**	

Katrina Mansfield,
Timothy Eveleigh,
Thomas H. Holzer, and
Shahryar Sarkani

In an effort to reduce costs and time to deploy mission capable unmanned aerial vehicles (UAV), the Department of Defense (DoD) has transitioned smart devices into the battlefield as portable, handheld UAV ground control stations (GCS) without adequate cybersecurity protection. While a number of threat model approaches have been published, they are outdated and fail to evaluate a complete system. This article develops a holistic threat model that analyzes the cybersecurity vulnerabilities within the communication network, smart device hardware, software applications, as well as the insider threat. Additionally, this article provides a risk-based threat profile of a DoD pilot UAV smart device GCS system. This model will fill the gaps in current threat model approaches, to provide the DoD with a tool to properly assess the threat environment of a UAV smart device GCS, and build layers of security into the system throughout the system development life cycle.

Keywords: *acquisitions; process improvement; best practices; standardization; innovation*

With the rapid advancement of technology and its popularity in the consumer market, smart phones and tablets are migrating to and changing the way we operate on the battlefield. In the past, the Department of Defense (DoD) has been reluctant to allow smart devices to be used in a battlefield environment without the capability to provide secure connections for classified communication (Dalton, 2012). However, the enhanced capabilities and benefits of these small, handheld devices for mission planning and data sharing have persuaded the DoD to accept the inherent risks of using improperly secured smart devices on the battlefield. In fact, a number of these portable handheld UAV GCS devices are now part of a series of DoD pilot programs (Pellerin, 2013).

Background

UAV remote sensors often collect large amounts of data to be sent near real-time over a communication network for interpretation; however, current secured legacy military communication networks cannot support the large capacity needed to make this effective. Ultra High Frequency (UHF) satellite communication networks have been used to support UAV communication network requirements, but availability is limited only to the highest priority users and therefore is not always a viable solution (Wilcoxson, 2013). Other secured military wireless networks may be readily accessible, but share the same performance issues: processing capacity and latency limitations (Hartman, Beacken, Bishop, & Kelly, 2011). As a result, the DoD has explored solutions in the private sector to meet the rapidly evolving UAV communication requirements risking the use of unsecured networks.

Commercial smart phones and tablets provide the high processing capability needed to control and process data from UAVs in a compact, light-weight, mobile, handheld device. Using smart device technology and supporting software apps, the DoD has taken the functionality of a traditional GCS and miniaturized it into a mobile, portable smart device. These apps provide near real-time avionics flight display, navigation systems, system health monitoring and prognostics display, imagery and position mapping, and data processing (Troiani, 2011). Using a Fourth Generation (4G) Long Term Evolution (LTE) commercial wireless network solution provides a wide spectrum bandwidth, ranging from 1.4 to 20 megahertz (MHz); increasing the availability and options for operational frequencies for deployment. 4G LTE also significantly reduces latency issues and provides peak data rate capabilities that feature near real-time data links with minimal interference from the UAV remote sensors (Hartman et al., 2011).

Several DoD pilot programs have been established to evaluate the technical capabilities of smart devices and demonstrate a proof of concept of the UAV smart device GCS. Previous research has explored cybersecurity threats to the UAV and the traditional GCS; however, little research has been done to explore what additional cyber threats have been encountered with the use of commercially available smart devices to command and control UAVs. Much of the technology and processes currently in development to secure the UAV smart device GCS system are not accompanied by a proper threat analysis. Current threat model tools are outdated and incapable of conducting a thorough threat analysis of an information system in its entirety, resulting in deploying inadequately secured devices to the battlefield, and increasing system and mission risk (Stango, Prasad, & Kyriazanos, 2009). Our research presents a recommended approach to conducting a threat model for information systems. By evaluating the vulnerabilities and threats to a DoD UAV within the parameters of a smart device GCS pilot program, both civilian and military UAV communities can benefit from the successful deployment of a properly secured UAV smart device GCS.

UAV Smart Device Case Study

Using a combination of Yin's Case Study Research approaches, the proposed threat model approach was developed to assess the security of the UAV smart device GCS (Yin, 2013). The first step involved a documentation review to assess the gaps in existing threat model approaches, followed by interviews to assess gaps in current government practices and the effectiveness of the proposed threat model. Lastly, direct observations of a pilot UAV smart device program were conducted to assess implementation of the proposed threat model.

Phase I: Threat Model Gap Analysis

The threat models currently being used are outdated and do not reflect advances in technology. Consequently, a number of gaps exist in the threat models being used to protect information systems. Threat models need to evolve with the technology and the associated threats (Stango et al., 2009). The gaps in the following sections address problems we found assessing a range of current threat models.

For the past 10 years, threat models have focused primarily on software applications. This focus is due in part to system failures and loss of data caused by software threats, including software viruses (Di & Smith, 2007). However, as technology has advanced in information systems, such as the UAV smart device GCS, threats are no longer limited to just software. Information systems today are comprised of hardware, software, and communication networks. Therefore, threats must be evaluated for the complete Unmanned Aerial System (UAS) within one single threat model to ensure the UAS is secured as a whole.

Little has been done in the development of threat models for hardware and communication networks, even though the number of attacks to hardware and communication networks has increased significantly with the advancement in technology and popularity of smart mobile devices (Wang, Streff, & Raman, 2012). Current hardware and communication threat models are tailored to specific systems or areas of interest. Recently, communication network threat models have been developed to address security concerns in personal networks; network jamming attacks; mobile ad hoc and sensor networks; and command, control, communications, computers and intelligence (C4I) security threats. Even fewer hardware threat models have been developed, only addressing hardware that has been compromised by malicious software logic and threats to storage systems. However, these areas of vulnerabilities have not been a major concern for the UAV community. Therefore, the need to improve upon these threat models has not existed.

With the exception of Clark et al. (2007), threat models have only addressed threats from malicious external attackers and not the internal threats and vulnerabilities that can arise from users or maintainers of the system. While system security is extremely important and must be maintained, the human factor is the biggest vulnerability in any system and is more critical than technology. Many of today's security problems are attributed to inadequate security awareness on the part of users and maintainers, yet the majority of threat models do not address the internal human factors that can compromise system security (Chen, Shaw, & Yang, 2006).

A number of threat model methodologies exist; each has been tailored to fit the needs of a specific user and/or area of interest. A crucial, but often omitted step required within a threat model approach is a threat analysis. A threat analysis involves assessing the risk and prioritizing each threat and then determining the countermeasures to enhance system security. Threat models that fail to complete a threat analysis are incomplete, and do not provide designers with the information required to properly secure the system (Oladimeji, Supakkul, & Chung, 2006).

Threat Model Comparison. Table 1 introduces six published threat models and highlights critical gaps in the approaches that each describes. The following discussion further elaborates on these models and the gaps within each.

TABLE 1. THREAT MODEL COMPARISON

Threat Model Gaps	UAV Smart Device GCS Threat Model	A Hardware Threat Modeling Concept for Trustable Integrated Circuits	Threat Modeling for Mobile Ad Hoc and Sensor Networks	Security Threat Modeling and Analysis: A Goal Oriented Approach	Enhanced C41 Security Using Threat Modeling	Cyber Security Threat Analysis and Modeling of a UAV System
Identifies and addresses software threats	X			X		X
Identifies and addresses hardware threats	X	X			X	
Identifies and addresses network threats	X		X		X	X

Risk analysis and threat prioritization	X			X		X
Identifies and addresses human (inside/external) threats	X		X			

A Hardware Threat Modeling Concept for Trustable Integrated Circuits proposes a threat model approach to identifying hardware threats "to determine a circuit's trustability and provide guidance to malicious-logic checking tools" (Di & Smith, 2007, p. 1). This threat model is a simplified approach that involves understanding what the adversary wishes to accomplish and possible entry points, as well as identifying threats and attacks to the digital integrated circuits. While the need to determine the severity of threats and attacks as discussed, the threat model fails to identify a recommended approach rendering this threat model approach to hardware incomplete. While identifying threats is important to the security of device, this threat model approach doesn't provide information to make a determination on how to proceed forward with securing the device.

Threat Modelling for Mobile Ad Hoc Sensors Networks, as demonstrated by Clark et al. (2007), introduces a threat-model approach for mobile ad hoc networks and sensor networks. This threat-model approach characterizes the network system based upon military operation modes in peace-time, transition to war, and wartime; recognizing the variations of system context and operation may impact the risk decision making. Focusing on the adversary, this threat model attempts to identify what capabilities the adversary may have that may present a threat to the communication network. Based upon the operational environment and adversary capabilities threats to the network communications, infrastructure and services, physical nodes and people are identified. This threat model addresses a need for a risk-management approach to make a determination for what threats pose the greatest risk and an approach to addressing those threats. The threat model, however, fails to identify or even mention the need for countermeasures.

Oladimeji et al. (2006), in their Security Threat Modeling and Analysis: A Goal-Oriented Approach, uses a negative softgoal or N-softgoal approach to identify threats to software applications. This simplified threat-model approach defines security objectives for the system, identifies software threats, analyzes threats and their associated risks, and provides a mitigation plan for countermeasures. This approach is effective for addressing software applications only.

Enhanced C4I Security Using Threat Modeling identifies a threat-modeling approach to C4I systems to protect sensitive military information being exchanged between information systems (Alghamdi, Hussain, & Faraz Kahn, 2010). The threat-model approach utilizes a variation of the negative softgoals approach described earlier in conjunction with the use of existing DoD architecture framework (DoDAF) artifacts. DoDAF operational view and system view diagrams are used to decompose and identify the operational needs of the system, interconnections, boundaries, scope, interfaces, entry and exit points, access points, attack points, and need lines. Using N-softgoal trees, threats and countermeasures to the system are identified based upon breaches to confidentiality, integrity, and availability security principles. The threat-model approach vaguely addresses the hardware threats, focusing primarily on the communication network. While the threat model identifies countermeasures for each system threat, the threat model fails to address a risk-analysis approach, thereby giving the impression that each mitigation technique or countermeasure should be implemented. Implementation of each countermeasure will not only drive up significant costs to the program but it may also impact the overall performance of the system.

Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System is intended to provide a threat model approach for a traditional UAV system; however, the threat-model approach focuses mainly on the communication link between the UAV and the traditional GCS (Javaid, Sun, Devabhaktuni, & Alam, 2012). The threat model identifies threat attacks to the confidentiality, integrity, and availability of the communication network, with mere acknowledgement of software threats to the UAV and GCS. A risk analysis is conducted of the communication network using flight simulation software; however, the approach fails to identify countermeasures and a mitigation plan. While the threat model discusses the components of the UAV system for background purposes, it is not considered part of the threat model and therefore may explain why the complete system is not assessed.

Threat modeling is a powerful tool that is critical to a system's security if used properly by the security team. Threat models provide the foundation on which threats will be identified, addressed, and mitigated. Table 1 identifies the gaps that exist within current threat models. Our proposed threat-model approach is the first research-based model that addresses the UAV smart device GCS while also addressing existing gaps in threat models and government security practices. This robust threat model for the UAV smart device GCS will fill the gaps identified in current threat models and improve on existing techniques by addressing threats to all areas of an information system (hardware, software, communication network, and people), and conducting a thorough threat analysis by completing a risk assessment and providing countermeasures for the threats identified.

The threat model should be implemented throughout the system development life cycle and other government processes to enhance the security of the UAV smart device GCS. Identified threats that pose the greatest risk must be addressed in the UAS's security requirements, since those risks cannot be allowed to manifest if system security is to be ensured. This will help ensure security is built into the system, making both the government and defense contractors responsible for implementing the overall security of the device. The system design, accordingly, is influenced by the countermeasures implemented to mitigate threats to the system (Myagmar, Lee, & Yurcik, 2005). Security testing is conducted based on threat analysis to ensure that the final UAV smart device GCS system will be protected from the threats identified prior to deployment and to prevent attacks once the UAV smart device GCS system is fielded (Wang et al., 2012). Once the system is deployed, the threat model will need to be updated to reflect the changing threat environment and changes to the UAV GCS and the UAS. These are made to ensure that system security is maintained.

> ***Poorly written security requirements that fail to hold the program manager or the defense contractor accountable for implementation of specific security parameters will be outweighed by costs, resources, mission requirements, time constraints and politics to meet the program schedule.***

Phase II: Conduct Interviews

Security gaps in government systems. Cybersecurity has become a major focus for both the defense and commercial industries due to the growing number of publicized cybersecurity breaches to both industries. While the government is making strides to address cybersecurity in both the workplace and battlefield, we must first understand where the gaps exist. Thirty information assurance and cybersecurity subject matter experts in areas of policy, certification and accreditation, design, implementation, and test evaluation were interviewed to evaluate the existing gaps in the DoD processes for cybersecurity. This group exposed trends and showed existing gaps in policy, personnel, and threat models.

Security policies have been written vaguely and are often open for interpretation. Implementation of these policies has been at the discretion of the program managers who may not completely understand what is required, and therefore fail to dedicate the personnel and financial resources. Poorly written security requirements that fail to hold the program manager or the defense contractor accountable for implementation of specific security parameters will be outweighed by costs, resources, mission requirements, time constraints, and politics to meet the program schedule. Once the system reaches information assurance accreditation and certification, the system design is complete and ready for deployment. The cost to address the security of a deployment-ready system is significantly higher than at the start of the program. As a result, the program manager will most often be forced by schedule constraints to accept the security risks to meet the program schedule, budget constraints, and warfighter need.

Information assurance and cybersecurity expertise over the years has been synonymous with security policies, accreditation, and certification; however, programs need cybersecurity subject matter experts that are also knowledgeable about the system (hardware, software, and communication networks), systems engineering, and test and evaluation processes. Ideally, security teams with this expertise will help to ensure all components of the system have been properly secured and addressed throughout the entire system development life cycle. However, the resources and personnel to support each respective program are often limited or not available. Accountability for properly securing the system has been the sole responsibility of the government; the government must sufficiently address the security of the system in the requirements section of the contract to enforce shared responsibility with defense contractors. This will help to build security into the system and fill the personnel gaps and expertise that currently exist within the government.

While threat models are being used by the DoD to evaluate cybersecurity vulnerabilities to military systems, no standard approach for threat modeling exists. Every program has a different perspective and definition of what a threat model is and how it is used. Threat models are often classified because of the type of data they collect (e.g., threats and vulnerabilities). As a result, threat models are frequently classified and not stored at operating locations and development sites, limiting their value to the program. This critical data, however, should be made available as a tool for both the program manager and the security team to address the cybersecurity vulnerabilities of the system and to build security into the system throughout the development life cycle.

Phase III: UAV Smart Device GCS Threat Model Pilot Program

While the use of UAV smart device GCS is intended to enhance the mission planning tools, environmental awareness, and operational capabilities of a multimillion-dollar UAV to support soldiers in the field, the security of the system must be evaluated and embedded into the system design for safe operation. Development and implementation of the robust threat model for the UAV smart device GCS is a key tool to ensure a secure and a safe operational environment.

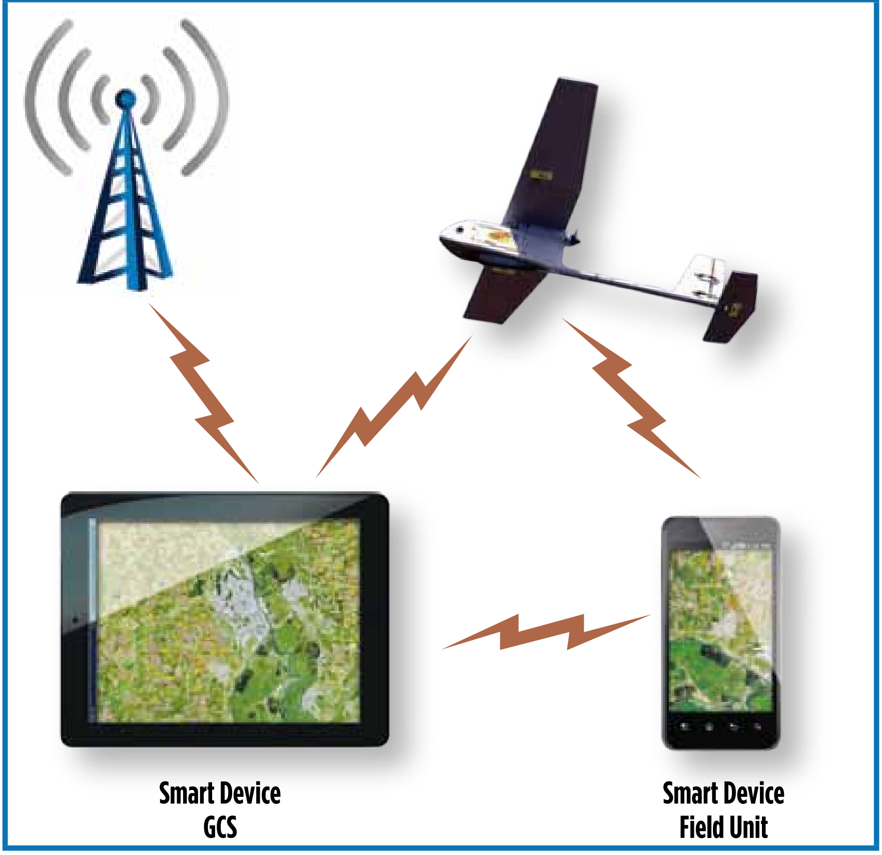
The robust threat model for the UAV smart device GCS is a seven-step process that will: (1) characterize the system, (2) understand the adversary's objectives, (3) identify system assets and vulnerabilities, (4) identify threats and attacks, (5) conduct threat analysis and prioritization, (6) identify countermeasures, and (7) determine the mitigation plan. The following discussion will elaborate on each step of the threat model approach using a DoD UAV smart device GCS pilot program for illustration in an unclassified, generalized manner to avoid discussion of sensitive data.

Step 1—Characterize the system. Characterizing the entire UAS is an important step in the threat modeling process, because it allows the security designer to understand the system and how it operates. While the overall goal of the threat model is to secure the UAV smart device GCS, the security countermeasures cannot hinder the functionality and the ability to meet mission capabilities and goals. Therefore, this step establishes the intended functional operation for the system and identifies the relationship of components in the UAV smart device GCS system that meets mission goals (Torr, 2005). While the primary focus is to secure the UAV smart device GCS, the functional operation of the device is dependent upon other external components within the system such as the UAV, communication network, and other field units.

The TigerShark UAV is a mid-endurance tactical UAV with weapon capability used to support military intelligence, surveillance, reconnaissance, target identification, and weapons' deployment missions. The UAV smart device GCS system for the pilot program has four major components (Figure): the TigerShark UAV, the smart device Android tablet GCS, the smart device field unit, and the LTE 4G communication network. Depending on the type of mission, the UAV may be flown using a preprogrammed flight plan uploaded to the onboard computer or flown by a remote pilot who relies solely on the GCS to command and control the UAV (Mirkarimi & Pericak, 2003). The GCS software is installed on a 19-inch Android tablet and is used to command and control the UAV and its payloads, providing real-time avionics flight display, navigation, system health monitoring and prognostics display, graphical images and position mapping, and inward data processing. Conveniently, the smart device field units can receive intelligence data from the smart device GCS or directly from the UAV. Lastly, the pilot program will utilize 4G LTE communication network technology to provide the high performance, high bandwidth network for enhanced capabilities, and the data networking requirements needed to receive and share near real-time data with the UAV smart device GCS.

> ***While the use of UAV smart device GCS is intended to enhance the mission planning tools, environmental awareness, and operational capabilities of a multimillion-dollar UAV to support soldiers in the field, the security of the system must be evaluated and embedded into the system design for safe operation.***

FIGURE 1. UAV—SMART DEVICE GCS SYSTEM FUNCTIONAL DIAGRAM



Step 2—Understand the adversary's objectives. The previous step (Characterize the System) established the components and functionality of the system to identify ways the adversary will want to attack the system. It is important to note that the previous step identifies mission and functionality goals, while this step establishes the security parameters of the system, keeping in mind that the mission, functionality, and security goals are all intertwined, and all are equally important in the threat assessment of the system.

To properly defend the system, one must view the system the way an adversary would. To succeed in blocking the impacts of enemy attacks, the security team must first identify the adversary's objectives. The key step here is to answer the question, what do the attackers want? (Myagmar et al., 2005). The output of this step will help to determine the vulnerabilities of the UAV smart device GCS in the next step.

The adversary's goal of attack on the smart device GCS is primarily to: (1) disrupt the operation of the device to prevent control of the TigerShark UAV, (2) gain control of the smart device GCS to control the TigerShark UAV, and (3) gain access to data that may be useful to the attacker. If the attacker is successful in any of these goals, the attacker can prevent completion of the mission (Yochim, 2010). These goals are often achieved through spoofing, tampering, repudiation, information disclosure, denial of service, and elevation-of-privilege attacks (Myagmar et al., 2005).

Step 3—Identify systems assets and their vulnerabilities. Using the information developed from the use case and adversary's objectives, this step identifies the assets and vulnerabilities specifically for the UAV smart device GCS system, which comprises the UAV smart device GCS and communication network only. An asset is an "abstract or concrete resource that a system must protect from misuse by an adversary" and is often an opportunity for attack (Myagmar et al., 2005, p. 3). Vulnerability is a security weakness or flaw that makes a system susceptible to attack (Oladimeji et al., 2006).

The UAV smart device GCS system is comprised of the hardware, software, and communication network components; therefore, we must assess these areas of vulnerability. Yet, we cannot properly assess the system without identifying vulnerabilities that are also introduced by the users and maintainers (Chirillo & Danielyan, 2005).

Hardware assets and vulnerabilities. The TigerShark UAV pilot program is utilizing an Android smart device tablet for the GCS. Hardware assets within the Android smart device tablet, such as the microphone, camera, and GPS, can be exploited to monitor the user and the users' surrounding environment (Delac, Silic, & Krolo, 2011). Memory storage can also contain classified information about the mission that can be useful to the attacker (Hasan, Myagmar, Lee, & Yurcik, 2005, pp. 94–102). Although the battery does not contain sensitive information, attackers can drain it to disrupt or terminate operation of the system (Delac et al., 2011). These threats can be introduced through malware software that enters through software and counterfeit hardware vulnerabilities.

Supply chain cybersecurity attacks have been a growing concern of the United States government since 2005, resulting in the seizure of large quantities of counterfeit network hardware and other information technology from Chinese telecommunication companies. Supply chain cybersecurity threats are introduced by hostile agents that purposefully install spyware into hardware components and/or alter circuitry with malicious firmware that is later sold to government and big businesses as counterfeit hardware (Goodwin, 2013). Once the electronic components are connected to the network, the enemy can easily gain access to it or, even worse, gain control of the electronic device to spy or cause harm. Unfortunately, many supply companies are transnational or the result of mergers, which makes it virtually impossible to adopt corporate ownership or control supply chain security of hardware components.

Another vulnerability is that enemies can gain physical access to the smart device GCS in a battlefield environment. A soldier under heavy fire can lose, drop, damage the device, or leave it behind in a life-and-death situation. The device can then be tampered with and analyzed to gain access to sensitive information stored in its memory.

Software assets and vulnerabilities. The heart of the smart device GCS is its mobile operating system, which controls its hardware resources and software applications. Infiltration of the operating system can be achieved through “jailbreaking,” whereby restrictions and security measures can be removed to allow users to modify the device and install software applications. Once the attacker has found a way inside the system, it is easy to manipulate the hardware resources and transform the smart device into a device for spying that will allow the attacker to capture images and video, tap and record conversations, view sensitive information, and gain the location of targeted individuals (Felt, Finifter, Chin, Hanna, & Wagner, 2011, pp. 3–14). The pilot program is utilizing a smart tablet with an Android operating system. The software code has been made publicly available to allow customization and modifications to meet the needs of the various smart device types and communication carriers. The open operating system has resulted in many variations of Android smartphones and tablets whereby different carriers with identical devices may have different variations of the operating system software. Google security updates are pushed to the system’s end users at the discretion of carrier and third-party application developers; depending on the complexity and time to make and test

> ***Software apps downloaded to the smart device are an easy target of cybersecurity attacks and must be protected by security mechanisms such as app certification or signature and pre-testing.***

modifications to tailor their devices, the carrier or third party software app developers may refuse to push the update to the end user, thereby increasing vulnerability to the smart devices (Rose, 2011).

Software apps provide the functionality of the GCS on smart devices. A successful attack on the software app could allow the attacker to gain control of the UAV functionality and access data gathered from the UAV, targeting individuals or locations for physical harm (Do, Kwon, & Moon, 2013).

Communication network vulnerabilities. In a tactical environment, ground soldiers are moving in a remote terrain where the coverage and performance of mobile networks are degraded and unsecure. Therefore, ground soldiers must provide their own secure, mobile networks to ensure continuous service (O'Rourke & Johnson, 2011). Stationary base stations establish a mobile network through a high-bandwidth, wired network backbone. However, if the ground soldiers move to another location, the mobile network is disrupted and inoperable until it is re-established.

Base stations are often attractive targets by hostiles desiring to disable the communication network. If the base station is destroyed, the secure communication network is inoperable, and ground soldiers will create their own insecure mobile networks or use insecure commercial networks. These actions introduce threats into the communication network, the devices operating on the network, and the missions they support (Bhargava, 2013). Direct attacks on the communication network can disrupt the connection between the UAV and the smart device GCS, thereby preventing operation and control of the UAV. They prevent the sharing of information within the UAV smart device GCS system; and potentially share information with other unauthorized users (Clark et al., 2007).

Human vulnerabilities. Threat models often focus on external attackers and threats that can affect the system. What tends to be overlooked, however, is how users and maintainers of the system also pose a danger to the system. Users can accidentally or intentionally share sensitive information or physically compromise the system by disregarding policies and operating procedures, or fail to update policies and procedures aimed at current threats (Clark et al., 2007). Although smart devices have been deployed in the battlefield to function as UAV GCSs, they can also be used for many other capabilities that may be of interest to the unwitting user and introduce threats to the GCS. For instance, users and operators could access social networks and e-mail outside of battlefield operations, thereby increasing the chances that phishing, spam, malware, and spyware will infiltrate the system (Leavitt, 2011).

Maintainers of the smart device GCS play a crucial role in its security and also determine the effectiveness of countermeasures implemented within the device. Poorly maintained systems expose entry points of attack to gain control of the UAV GCS (Whitman & Mattord, 2010).

Step 4—Identify threats and attacks. Using the information gathered in the previous step, the next step is to identify threats and attacks to the system. As previously mentioned, a threat is defined as a "potential violation of the security of a system, an event that may have some negative impact," and an attack is an "exploitation of a vulnerability to realize a threat" (Oladimeji et al., 2006, p. 1). The threat identification process described in the following discussion examines threats in detail for four areas of vulnerabilities.

Hardware threats. Threats to the Android smart device GCS hardware include attacks that cause battery exhaustion, flooding, surveillance, and USB and storage attacks. Battery exhaustion attacks cause the battery to discharge faster than normal, killing the smart device and ultimately disabling the GCS. This prevents the operation and control of the UAV. Flooding attacks disable the smart device by overloading it with numerous signals or messages, preventing GCS operation or preventing it from providing or receiving information within the network (Bhusari & Sahu, 2013). Surveillance attacks employ smart device sensors to monitor the surrounding environment and soldier movement, which allows the attacker to gain unauthorized access to mission information and identify the location of the soldier maneuvering the UAV and other soldiers nearby. Storage snooping attacks, a result of malware, allow the attacker to gain access to sensitive information via storage snooping attacks. Storage jamming and alteration attacks modify data for the purpose of subverting, degrading, or disrupting operations (Hasan et al., 2005).

Software threats. Mobile platforms resemble traditional desktop operating systems; therefore, the security threat profile of a personal computer has migrated to smart devices (Delac et al., 2011). Malware attacks gain access to a device to steal data, damage the device, or annoy the user. This threat includes Trojan horses, botnets, worms, key loggers, and rootkits (Felt et al., 2011). In addition, malware can be used to disrupt and gather sensitive information or obtain control of the GCS and UAV. Spyware collects personal information such as location and stored information (Felt et al., 2011). It can also be used to gather intelligence from UAV real-time data feeds or directly from the smart device GCS using the microphone, camera, GPS, or stored data to obtain mission-sensitive information. Data accessed by malware and spyware attacks can introduce data leakage and unauthorized data transmission. Malicious software also can be used to tamper with data by either destruction or modification (Bhusari & Sahu, 2013). Sensitive information or dangerous capabilities are often protected by requiring user consent before an application can gain access. However, elevation of privilege is a common attack achieved through software manipulation to gain access to resources that would otherwise be protected (Olzak, 2006).

Communication network threats. Threats to the communication network include network eavesdropping, spoofing, denial of service, impaired quality of service, jamming, weak/compromised cryptography, and unencrypted communication. Network eavesdropping or sniffing captures and decodes packets as transmitted over the network. Spoofing attacks masquerade the hacker as a trusted party in the network to gain access to sensitive information, which can lead to data leakage—the unauthorized transmission of sensitive data. Denial of service or network congestion overloads a link or node in the UAV smart device GCS system with an extensive amount of data to reduce the quality of network performance or cause denial of service (Spiewak, Engel, & Fusenig, 2006, pp. 35-40). Impaired quality of services, another form of denial of service, is an attack that degrades the level of performance or causes disruption of the network to prevent services required for applications, users, or data flow (Clark et al., 2007). Denial of service attacks not only threaten the communication network, but also the UAV. False commands or control signals transmitted over the network to the UAV can make the UAV land or attack somewhere else (Javaid et al., 2012). A jamming device can disrupt and disable communication between the smart device GCS and UAV, and other components in the network, thereby preventing control of the UAV and dissemination of information within the network hub. Weak cryptographic algorithms are easily broken by attackers exposing sensitive data to adversaries. If the attacker intercepts the encryption key, the cryptography becomes compromised, and the network is exposed to data leakage. Sharing sensitive information using unencrypted communications allows for harmful data leakage to unauthorized parties (Clark et al., 2007).

Human threats. Threats to the UAV smart device GCS can also be introduced by system users and maintainers. In some instances, threats will enter the system due to careless mistakes or inadequate practices, such as the failure to follow policies or inadequate policies, use of unencrypted communication, carelessness with cryptographic keys, poor risk decisions, and poor management or maintenance. These threats can lead to data leakage, entry of erroneous data, accidental deletion or modification of data, storage of data in unprotected areas, and failure to protect information (Whitman & Mattord, 2010). Poor risk decisions can be the result of carelessness or a combination of poor training and the stress and limitations of completing missions in a battlefield environment. Insufficient management and maintenance of the GCS can compromise system integrity, hinder GCS performance, and even render it inoperable (Clark et al., 2007).

Compromised personnel acting as inside agents are another vulnerability. They can introduce threats such as harmful data leakage and could modify stored accountability information. Obvious threats from an inside agent include directing the GCS and UAV to conduct surveillance on and attack military personnel. Access to the GCS could also provide sensitive data to adversaries and lead to the destruction of sensitive data. Accountability information is extremely important in military applications, as users and maintainers are responsible for operating and maintaining a device that controls multimillion-dollar unmanned aircraft with weapon capabilities. In the event that an error occurs, poor decisions are made, or the device is compromised, accountability logs can be reviewed post-operation to connect actions to people. Accountability logs can be attacked by preventing the collection or storage of accountability information. By the same token, deletion and modification of accountability information to shift blame or render it impossible to determine blame also has a negative effect on security (Clark et al., 2007).

Step 5—Conduct threat analysis and prioritization. The previous steps help to identify threats to UAV smart device GCSs. The next step analyzes threats by completing a thorough risk assessment of each threat to prioritize the threats and address countermeasures for high-risk attacks (Myagmar et al., 2005).

While it is impossible to guarantee 100 percent security of a system, it is important to identify the threats, prioritize their associated risks, and identify those that are most crucial for the UAV smart device GCS operational environment (Oladimeji et al., 2006). To assess the risk of identified threat attacks, the likelihood and impact are calculated using the National Institute of Standards and Technology (NIST) Management Guide for Information Technology Systems methodology (Stoneburner, G., Goguen, A., & Feringa, A., 2002). NIST is the designated authority for the development of information security standards and guidelines for federal government agencies and private industry. Since the UAV smart device GCS operational environment is being evaluated for military purposes, the NIST methodology is appropriate for assessing the risk and applied as follows.

Likelihood determination. The likelihood is the probability that a potential vulnerability will occur in the associated threat environment and considers threat-source motivation and capability, nature of the vulnerability, and the existence and effectiveness of current countermeasures (Stoneburner, Goguen, & Feringa, 2002). The following NIST criteria are used to rate the likelihood of the threats identified (Table 2).

TABLE 2. LIKELIHOOD DEFINITIONS

Likelihood Level	Likelihood Definition
High (1.0)	The threat source is highly motivated and sufficiently capable; controls meant to prevent the vulnerability from being exercised are ineffective.
Medium (0.5)	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low (0.1)	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Impact assessment. The impact assessment determines the level of impact to system assets and sensitive data based on protections required to maintain security goals (Stoneburner, Goguen, & Feringa, 2002). The following criteria are used to rate the impact of the threats to the handheld, portable GCS (Table 3).

TABLE 3. IMPACT DEFINITION

Magnitude of Impact	Impact Definition
High (100)	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium (50)	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low (10)	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Threat risk assessment results. Using the likelihood and impact criteria, analyzed threats to the UAV smart device GCS system (Table 4) with a team of cybersecurity and system subject matter experts. Likelihood was assessed using existing threat data. Current research, experience, vulnerabilities, and the ability of existing controls to minimize vulnerabilities to the TigerShark UAV smart device GCS were included in the evaluation. Impact was assessed based on effect on mission goals and objectives, physical damage to assets and resources (UAV, GCS, etc.), and potential death or injury to humans. The risk for each threat was calculated as the product of the impact and likelihood, and risks were assessed at the following NIST defined levels: High Risk (product value >50 to 100), Medium Risk (product value>10 to 50), and Low Risk (1 to 10) (Stoneburner, Goguen, & Feringa, 2002).

TABLE 4. RISK ANALYSIS SUMMARY

Threat	Likelihood	Impact	Risk
HARDWARE			
Battery Exhaustion	0.5	100	50
Flooding	1.0	50	50
Surveillance	1.0	100	100
USB	0.1	10	1
Storage Snooping	0.5	50	25
Storage Jamming	0.5	10	5
Storage Erasure/Alteration	0.1	50	5
SOFTWARE			
Malware	1.0	100	100
Phishing	0.5	50	25
Data Leakage	1.0	50	50
Spyware	1.0	100	100
Data Tampering	1.0	50	50
Elevation of Privilege	1.0	100	100
COMMUNICATION NETWORK			
Eavesdropping	1.0	100	100
Spoofing	0.5	100	50
Denial of Service	1.0	100	100
Jamming	1.0	10	10
Weak/Compromised Cryptography	0.5	50	25
Unencrypted Communication	0.1	50	5
Impaired Quality of Service	0.5	100	100
HUMAN			
Breaking Policy	1.0	100	100
Inadequate Policy	1.0	100	100
Unencrypted Communication	0.5	50	25
Carelessness with Cryptographic Keys	1.0	50	50
Harmful Data Leakage	0.5	50	25
Compromise of Personnel	0.5	100	50
Poor Risk Decisions	0.5	100	50
Poor Management/Maintenance	1.0	100	100
Overloading the Operator	0.5	10	5
Prevention of Accountability from Being Stored	0.1	10	1
Destruction of Accountability Data	0.1	10	1
Modification of Accountability Data	0.1	10	1

Based on the above criteria, the risk assessment in Table 4 shows that surveillance attacks to the hardware, malware, and spyware attacks to the software; eavesdropping, denial of service, and impaired quality of service attacks to the communication network; and neglected or inadequate policy and poor management and maintenance practices pose the greatest risk to the UAV smart device GCS system. Of all these, malware is the most significant threat, because its likelihood is extremely high. The communication network is an important component to the UAS operation. As previously mentioned, the UAV smart device GCS pilot is utilizing 4G LTE network technology, a commercial communication network. While use of the 4G LTE network provides the communication network requirements for UAS operation in the battlefield, it doesn't provide the security of legacy military systems, thus increasing the risk of eavesdropping, denial of service, and impaired quality of service attacks. While there are solutions to secure the network during operation, performance degradation of the smart device GCS is an issue. Neglected or inadequate policies are a major vulnerability for UAV smart device GCSs. Neglected or inadequate policy can place the operator and other friendly forces on the battlefield in danger and compromise the security of the GCS and UAV. Poor management or maintenance of the UAV smart device GCS can weaken countermeasures embedded in the system and increase the risk of new threats to the UAS. These significant risks to the system should be given high priority and addressed with countermeasures.

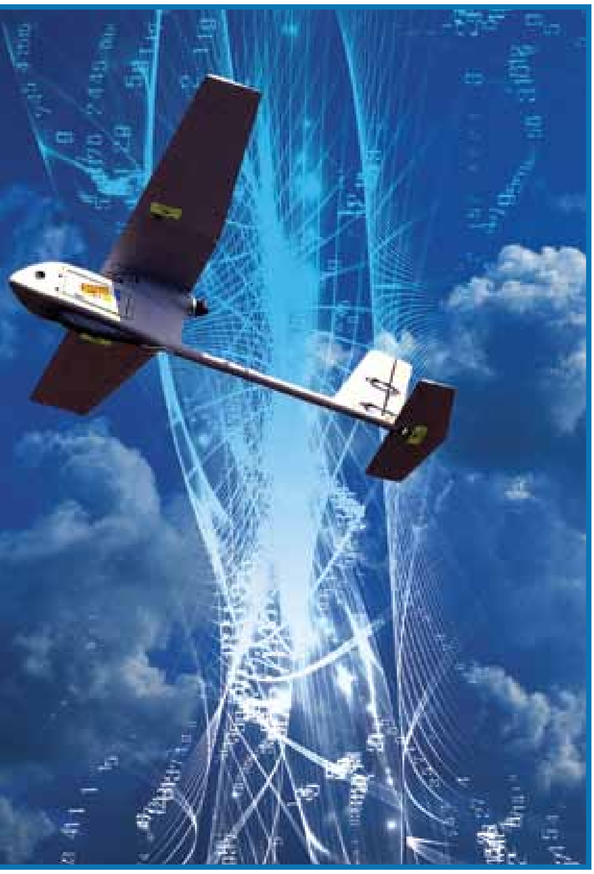
Medium-high risk threats that require countermeasures include battery exhaustion and flooding attacks to hardware; data leakage and surveillance attacks to software; data tampering, and spoofing attacks to the communications network; and compromised personnel, poor management, and poor risk decisions. The military must evaluate the remaining threats, which include those of medium and low risk, and determine whether to implement countermeasures, based on performance and cost factors, or accept the risk.

Step 6 – Identify Countermeasures. Countermeasures are "techniques to protect the system" (Alghamdi et al., 2010, p. 3). This step identifies countermeasures to counteract the medium- and high-risk attacks to the UAV smart device GCS identified in the last step. While a number of countermeasures will be identified to reduce risk to the system, all countermeasures cannot be implemented due to costs and performance degradation. Outputs from the threat analysis in the previous step will help to determine the combination of countermeasures for optimal protection with performance and costs.

Hardware countermeasures. U.S. companies and agencies can reduce risk to counterfeit networking hardware by limiting purchases to trusted vendors. Companies can also conduct random tests on devices during the distribution and installation phases to determine whether they contain extra components or serious vulnerabilities (Lee & Rotoloni, 2012).

A Smart device GCS obtained by the adversary can be counteracted with security mechanisms such as authentication, encryption, and remote wipe. These techniques can protect against unauthorized access to classified or sensitive information. Authentication limits access and privileges to only authorized parties, detecting and preventing access by others. This can also be achieved with passwords and screen lock codes; however, they can hinder the quick response and performance of soldiers using the devices on the battlefield. Encryption encodes data to prevent disclosure of sensitive or classified data to unauthorized parties. It can also protect data at rest (i.e., files, memory, USB flash drives, etc.) when physical security fails (Wang et al., 2012). Meanwhile, remote wipe allows the smart device GCS to be commanded remotely. Therefore, it can be reset or, if the device falls into an unauthorized user's possession, stored data can be erased. This security mechanism can be evaded, however, by removing the battery or memory card prior to receiving the remote wipe command (Hasan et al., 2005).

Software countermeasures. Malware and spyware are the most common attacks to operating system software and software applications, and can have major consequences if not detected immediately. Frequent testing for malware can be done using fuzz testing and static-analysis code scanning test tools. Fuzz testing sends structured, invalid inputs to software application programs and network interfaces to detect errors that can lead to software vulnerabilities. Static-analysis code scanning test tools can detect specific kinds of coding flaws and software vulnerabilities (Lipner, 2004). The smart device GCS can also be protected using antivirus and firewall software. Antivirus software can prevent, detect, and remove malware from software applications and operating system software, whereas a firewall can prevent unauthorized access to and from the smart device GCS and access to unauthorized, untrusted wireless networks. Software applications often access hardware resources within the smart device beyond what is required for operation of the app, increasing vulnerability of the smart device GCS. Access control limits accessibility to resources and/or services, only allowing the app to tap into the minimum resources needed (Jeon, Kim, Lee, & Won, 2011). Resource management monitors the availability and condition of resources (Shabtai et al., 2010).



Although smart devices will be used primarily as UAV GCSs, soldiers may be tempted to access personal e-mail and social networks, thereby introducing threats such as spam and phishing. Communication from outside the secure network should be blocked. Spam filters can also be used to prevent receipt of spam from unwanted parties via multimedia message service, text messages, e-mail, and telephone (Jeon et al., 2011).

Software apps downloaded to the smart device are an easy target of cybersecurity attacks and must be protected by security mechanisms such as app certification or signature and pre-testing. Application signatures should be used to ensure that the software is from a trusted source and has not been tampered with. Pretesting software apps by detecting malicious malware prior to use in the battlefield ensures that only secure apps will be uploaded to the software app database (Jeon et al., 2011).

Vulnerabilities to the software can be mitigated by regularly updating the operating system and software applications immediately after updates are released (Jeon et al., 2011).

Communication network countermeasures. Many threats to UAV smart device GCSs arise from deficiencies in network security. Flooding, jamming, denial of service, and impaired quality of service attacks can be mitigated by bandwidth allocation, which limits bandwidth for the smart device to prevent excessive connection request attacks that may impair network and affect the operation of the smart device

GCS. Eavesdropping and data leakage can be prevented by network encryption, which encodes data to prevent disclosure of sensitive data to unauthorized parties and can protect data in transit over shared networks. However, encryption policies and procedures must be updated periodically to ensure an adequate level of cryptography. Data transferred over the network can be protected by safe http data-transfer protocols, authentication certificates, data encryption and decryption, and virtual private networks (Markelj & Bernik, 2012). UAV GCS software requires consistent network access, but other software apps that support military operations may not (Clark et al., 2007).

In the past, network security concerns have hindered widespread smart phone deployment on the battlefield, but since 2010, the DoD has moved to enhance communication networks to accommodate the requirements for smart devices and UAV capabilities on the battlefield (Edwards, 2012). Stationary base stations, as previously discussed, didn't provide the infrastructure required for smart devices and UAVs, and therefore were inadequate for the current technology and enhanced capabilities (O'Rourke & Johnson, 2011). New technology advancements, such as mesh networks, mobile ad hoc networks, cognitive radios, and satellite communications have offered better options for mobile network availability on the battlefield. Mesh networks or mobile ad hoc networks provide high bandwidth networking capabilities to connect multiple smart devices within a specified range, control UAVs, and disseminate data feeds within the communication network. Cognitive radios can adapt to user needs and bandwidth conditions, providing quality system performance in all types of terrain. They are also resistant to eavesdroppers and jammers (Edwards, 2012). Advances in technologies such as antenna design and signal reception have made satellite communication networks a viable solution for smart devices on the battlefield. Satellite communication is ideal for coverage of terrestrial areas (Varshney & Vetter, 2000).

The effectiveness of countermeasures previously identified depends on the actions taken by users and maintainers to secure the system. Security countermeasures for the GCS can be significantly enhanced through security policies, education, training, and awareness (Chen, Shaw, & Yang, 2006). To reduce the risk of data leakage, policies and operating procedures should be updated periodically to reflect current mission requirements and threats. Security policy is important, as it defines the rules, guidelines, and procedures for proper use and protection of the system (D'Arcy, Hovav, & Galletta, 2009). In addition to updating policy, users and maintainers must be made aware of all changes in policies and procedures, and be educated and trained periodically to stay abreast of the most up-to-date information. This will also make users and maintainers accountable for their actions on the battlefield. Security education, training, and awareness provide users and maintainers with information regarding the security environment and the skills required to perform security procedures and reinforce security policy awareness and comprehension (D'Arcy et al., 2009). These should address information security policy, system access control, system development and maintenance, personnel security, physical and environmental security, security organization, asset classification and control, communications and operations management, business continuity management, and compliance (McAdams, 2004).

Maintenance of the smart device GCS is essential for their security. Updates, upgrades, and patches are especially important, as they increase protection from known cybersecurity threats and reduce risks to vulnerabilities in software code in the operating system and software applications. Smart device hardware must also be evaluated and maintained to ensure system effectiveness and ability to meet mission requirements. If the system is deemed ineffective or no longer meets the mission requirements, the devices should be disabled and properly disposed of (Whitman & Mattord, 2010).

To prevent human error or to block compromised personnel from gaining control of the device, controls or safeguards should be implemented. Strong authentication safeguards can be as simple as entering a command twice; having another party verify a command before

> ***If designers are not careful, they can go too far in designing countermeasures and render them more expensive than they are worth.***

implementation; using passwords, smart card, personal identification numbers, and/or a form of biometrics verification (Whitman & Mattord, 2010).

Step 7 – Determine the mitigation plan. In the previous steps, risk was assessed to identify high-priority threats that should be mitigated and countermeasures were identified to block the attacks to the UAV smart device GCS. Once the threat-attacks have been assessed and prioritized, they must be managed by assuming, controlling, transferring, or avoiding the risk. A risk should be assumed if the risk is low and the cost to mitigate is sufficiently high; it can also be transferred to another user via warnings, etc. If a system component or feature associated with a risk is too costly to mitigate or the risk is too high to accept, the risk can be avoided by removing the relevant component or feature. Lastly, a risk can be controlled with countermeasures (Myagmar et al., 2005). If designers are not careful, they can go too far in designing countermeasures and render them more expensive than they are worth. The cost to implement a countermeasure must be factored into the design decision and should not exceed the expected risk (Oladimej et al., 2006).

While cost is an important factor, countermeasures must also be evaluated based on the ability to meet mission goals and offer operational benefits. The UAV smart device GCS is being evaluated for military operations; therefore, countermeasures must enable mission accomplishment with tolerable risk and reflect the environment in which the system is deployed (Clark et al., 2007).

Conclusions

As technology continues to progress, the U.S. government cannot afford to sacrifice security for enhanced capabilities and features on the battlefield. Mission success is always the top priority, but not at the cost of compromising sensitive information, loss of multimillion-dollar assets, or casualties of soldiers. While a number of threat models exist, they have not evolved to effectively evaluate today’s technology. Current threat models: (1) focus primarily on software applications, and don’t address threats to the system in totality—hardware, software, and communication network, (2) only address the adversary and fail to address the insider threat—users and maintainers of the system, and (3) fail to provide a threat analysis that assesses the risk, prioritizes the threats, and provides countermeasures. The robust threat model we propose for the UAV smart device GCS has filled the gaps identified in current threat models and has improved on existing techniques by addressing threats to a complete UAS (hardware, software, communication network) and the associated human threats. Our approach also conducts a thorough threat analysis by completing a risk assessment and provides countermeasures for the threats identified. This comprehensive threat model analysis will help designers and users in the military and civilian UAV communities to understand the threat profile of their system and to enhance the security and operational environment of the UAV smart device GCS. Most importantly, the secured devices will provide soldiers with the secure, enhanced mission capabilities needed to protect soldiers in the battlefield.

While this threat model analysis addresses threats to military UAV smart device GCSs, the enhanced threat model can also be used to assess Federal Aviation Administration civilian UAV GCSs and industry applications that use smart devices for the reception and sharing of sensitive information. As technology continues to advance, adversaries will continue to alter their cyber footprint. Governments and industry agencies must adapt accordingly and assess threats effectively. Our model holds the key to the future of security.

References

Alghamdi, A. S., Hussain, T., & Faraz Khan, G. (2010, March). *Enhancing C4I security using threat modeling*. Proceedings of 12th International IEEE Conference on Computer Modelling and Simulation (UKSim) (pp. 131–136), Cambridge, UK, March 24-26.

Bhargava, B. (2013). *Security in mobile networks*. Retrieved from cs.brown.edu/nsfmobile/nsf-contextaware.doc

Bhusari, M. V. K., & Sahu, M. A. M. (2013). Smartphone attacks and security challenges. *International Journal of Computer Science and Management Research*, 2(5), 2473–2476.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning & Performance Journal*, 24(1), 1–14.

Chirillo, J., & Danielyan, E. (2005). *Sun certified security administrator for Solaris 9 & 10 study guide*. Boston, MA: McGraw-Hill.

Clark, J. A., Murdoch, J., McDermid, J., Sen, S., Chivers, H., Worthington, O., & Rohatgi, P. (2007, September). *Threat modelling for mobile ad hoc and sensor networks*. Proceedings of Annual Conference of International Technology Alliance (ACITA) (pp. 25–27), Hyattsville, MD, September 25–27.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98.

Delac, G., Silic, M., & Krolo, J. (2011, May). *Emerging security threats for mobile platforms*. Proceedings of the 34th International Convention, MIPRO 2011 (pp. 1468–1473), Opatija, Croatia, May 23–27.

Di, J., & Smith, S. (2007, April). *A hardware threat modeling concept for trustable integrated circuits*. Proceedings of IEEE Region 5 Technical Conference (pp. 354–357), Fayetteville, AR, April 20–21.

Do, T. D., Kwon, J., & Moon, C. J. (2013). Ground system software for unmanned aerial vehicles on android device. *World Academy of Science, Engineering and Technology*, 74, 718–723.

Edwards, J. (2012). *The future of military comms on the battlefield*. Retrieved from http://defensesystems.com/articles/2012/02/08/cover-story-military-communications-technologies.aspx

Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). *A survey of mobile malware in the wild*. Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM 2011). New York: Association of Computing Machinery.

Goodwin, B. (2013). *IT manufacturers fight cyber espionage risks in the supply chain*. Retrieved from http://www.computerweekly.com/news/2240181320/IT-manfuctürers-tackle-cyber-espionage-risks-in-the-supply-chain

Hartman, A. R., Beacken, M. J., Bishop, D. J., & Kelly, K. L. (2011, November). *4G LTE wireless solutions for DoD systems*. Proceedings of the 2011 IEEE Military Communications Conference (MILCOM 2011) (pp. 2,216–2,221), San Diego, CA, November 7–10.

Hasan, R., Myagmar, S., Lee, A. J., & Yurcik, W. (2005). *Toward a threat model for storage systems*. Proceedings of the 2005 ACM Workshop on Storage Security and Survivability. New York: Association of Computing Machinery.

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. (2012, November). *Cyber security threat analysis and modeling of an unmanned aerial vehicle system*. Proceedings of IEEE International Conference on Technologies for Homeland Security (HST) (pp. 585-590), Waltham, MA, November 13–15.

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011, July). *A practical analysis of smartphone security*. Proceedings of the 2011 International Conference on Human interface (HI '11) and the Management of Information (Vol. I, pp. 311–320), Orlando FL, July 9–14.

Leavitt, N. (2011). Mobile security: Finally a serious problem? *Computer*, 44(6), 11–14.

Lee, W., & Rotoloni, B. (2012). *Emerging cyber threats report 2013*. Retrieved from http://www.gtcybersecuritysummit.com/pdf/2013ThreatsReport.pdf

Lipner, S. (2004, December). *The trustworthy computing security development lifecycle*. Proceedings of IEEE 20th Annual Computer Security Applications Conference (ACSAC) 2004 (pp. 2–13), Los Alamitos, CA, December 6–10.

Markelj, B., & Bernik, I. (2012). Mobile devices and corporate data security. *International Journal of Education and Information Technologies*, 6(1), 97–104.

McAdams, A. C. (2004). Security and risk management: A fundamental business issue. *Information Management Journal–Prairie Village*, 38(4), 36–45.

Mirkarimi, D. B., & Pericak, C. (2003). Countering the tactical UAV threat. US Armor Association, 112(1), 43–44.

Myagmar, S., Lee, A. J., & Yurcik, W. (2005, August – September). *Threat modeling as a basis for security requirements*. Proceedings of 13th IEEE International Requirements Engineering (RE) Conference, Symposium on Requirements Engineering for Information Security (SREIS), Paris, France, August 29–September 2.

Oladimeji, E. A., Supakkul, S., & Chung, L. (2006, November). *Security threat modeling and analysis: A goal-oriented approach*. Proceedings of 10th International Association of Science and Technology for Development (IASTED) International Conference on Software Engineering and Applications (SEA 2006) (pp. 13-15), Dallas, Texas, November 13–15.

Olzak, T. (2006). *A practical approach to threat modeling*. Toledo, OH: Erudio Security, LLC.

O'Rourke, C., & Johnson, S. B. (2011). *Mobile ad hoc networking revamps military communications*. Retrieved from http://www.cotsjournalonline.com/articles/view/102158

Pellerin, C. (2013). *DARPA pioneers tactical mobile devices for soldiers*. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=121320

Rose, C. (2011). Smart phone, dumb security. *Review of Business Information Systems (RBIS)*, 16(1), 21–26.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S., & Glezer, C. (2010). Google android: A comprehensive security assessment. *IEEE Security and Privacy*, 8(2), 35–44.

Spiewak, D., Engel, T., & Fusenig, V. (2006). *Towards a threat model for mobile ad-hoc networks*. Proceedings of the 5th WSEAS International Conference on Information Security and Privacy (ISP'06). Stevens Point, WI: World Scientific and Engineering Academy and Society.

Stango, A., Prasad, N. R., & Kyriazanos, D. M. (2009). *A threat analysis methodology for security evaluation and enhancement planning*. Proceedings of IEEE Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2009) (pp. 262–267), Athens, Greece, June 18-23.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Torr, P. (2005). Demystifying the threat modeling process. *Security & Privacy*, 3(5), 66–70.

Troiani, G. (2011). DARPA looking to develop mobile devices to command UAVs. *ExecutiveBiz®*. Retrieved from http://blog.executivebiz.com/2011/12/darpa-looking-to-develop-mobile-devices-to-command-uavs

Varshney, U., & Vetter, R. (2000). Emerging mobile and wireless networks. *Communications of the ACM*, 43(6), 73–81.

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges. *Computer*, 45(12), 52–58.

Whitman, M. E., & Mattord, H. J. (2010). *Principles of information security*. Boston, MA: Cengage Learning.

Wilcoxson, D. (2013, November). *Advantages of mobile broadband communications services for military applications*. Proceedings of the 2013 IEEE Military Communications Conference (MILCOM 2013) (pp. 266–272), San Diego, CA, November 18–20.

Yin, R. K. (2013). *Case study research: Design and methods*. Thousand Oaks, CA: Sage Publications.

Yochim, J. A. (2010). T*he vulnerabilities of unmanned aircraft system common data links to electronic attack*. Ogden, UT: Weber State University.

Author Biographies

Ms. Katrina M. Mansfield is an engineering management and systems engineering doctoral student at The George Washington University. She has worked for the Department of Defense for the past 7 years supporting operation and integration of avionics devices in naval aircraft. Ms. Mansfield has an MS in Engineering Management from Johns Hopkins University and a BS in Electrical Engineering from Morgan State University.

(E-mail address: kmansfi@gwu.edu)

Dr. Timothy J. Eveleigh is an adjunct professor of engineering management and systems engineering at The George Washington University and an International Council on Systems Engineering (INCOSE) Certified Systems Engineering Professional. Dr. Eveleigh has over 30 years' industry experience working DoD/intelligence community information technology acquisition challenges, research and development, and enterprise architecting. Dr. Eveleigh has enjoyed a 30-year parallel career as an Air Force Reserve intelligence officer and developmental engineer focused on command and control integration.

(E-mail address: eveleigh@gwu.edu)

Dr. Thomas H. Holzer is an adjunct professor of engineering management and systems engineering at The George Washington University. He was the director, Engineering Management Office, National Geospatial-Intelligence Agency, with 35 years' experience in systems engineering and leading large-scale information technology programs. Dr. Holzer holds a Doctor and Master of Science in Engineering Management from The George Washington University and a Bachelor of Science in Mechanical Engineering from the University of Cincinnati.

(E-mail address: holzert@gwu.edu)

Dr. Shahryar Sarkani is an adjunct professor in the Department of Engineering Management and Systems Engineering at The George Washington University. He has over 20 years of experience in the field of software engineering. Dr. Sarkani holds a Doctor of Science in Systems Engineering from The George Washington University, a Master of Science in Mathematics from University of New Orleans, and a Bachelor of Science in Electrical Engineering from Louisiana State University.

(E-mail address: emseor2003@yahoo.com)